Claims

The invention claimed is:

1. A method for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N, and where $E = \sum_{i=0}^{t} e_i 2^i$, and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that $mk \geq n + 2$, said method comprising the steps of:

providing a signal representing the constant, C, which is equal to 2^{+2mk} mod N;

multiplying said value A by said constant C using a circuit which accepts two input operands and which produces an output result value Z_0 given by $A\ C\ 2^{-mk}$ modulo N;

storing said value Z_0 in a first register and in a second register;

for sequential values of an index i running from 1 to t, repeatedly using the value in said second register as both of said operands for said circuit, with the output of said circuit being stored back into said second register and, when e_{t-i} is 1, using again the contents of said second register as one input operand to said circuit with said other input operand being said Z_0 value in said first register with the output of said circuit being stored in said first register;

upon completion of said repetition, operating said circuit with the contents of said second register as one input operand with the constant 1 as said other input operand; and

storing the output of said circuit in at least one of said said registers , whereby said at least one register contains the binary representation of A^E modulo N.

2. The method of claim 1 in which said final storing step stores the result in said second register.

3. A method for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N, and where $E = \sum_{i=0}^{t} e_i 2^i$, and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that $mk \geqslant n + 2$, said method comprising the steps of:

providing a signal representing the constant, C, which is equal to 2^{+2mk} mod N;

multiplying said value A by said constant C using a circuit which accepts two input operands and which produces an output result value Z_0 given by $A\ C\ 2^{-mk}$ modulo N;

storing said value Z_0 in a first register;

if $e_0 = 1$, storing the value 1 in a second register, otherwise storing the contents of said first register in said second register;

for sequential values of an index i running from 1 to t, repeatedly using the value in said first register as both of said input operands for said circuit, with the output of said circuit being stored back into said first register and, when e_i is 1, using again the contents of said first register as one input operand to said circuit with said other input operand being the contents from said second register and storing the result in said second register;

upon completion of said repetition, operating said circuit with the contents of said second register as one input operand with the constant 1 as said other input operand; and

storing the output of said circuit in at least one of said registers , whereby said at least one register contains the binary representation of A^E modulo N.

4. The method of claim 3 in which said final storing step stores the result in said second register.

5. A method for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N, and where $E = \sum_{i=0}^{t} e_i 2^i$, and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that $mk \geqslant n + 2$, said method comprising the steps of:

repeatedly operating, for at most t cycles, a circuit which computes $F\ G\ 2^{-mk}$ modulo N for binary input operands F and G to said circuit, with said circuit inputs being controllably selected, during each repetition, from the constant *1*, the constant 2^{+2mk} modulo N and the previous output from said circuit so as to produce an output of $A^E\ 2^{+mk}$ modulo N;

operating said circuit with one input being the output from said repeated step and the other input being the constant *1*, whereby the output of said circuit, after at most t cycles, is A^E modulo N.

6. An apparatus for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N, and where $E = \sum_{i=0}^{t} e_i 2^i$, and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that $mk \geqslant n + 2$, said apparatus comprising:

a circuit having two input operands for signals representing binary numbers F and G and which produces as a result the binary representation of $F\,G\,2^{-mk}$ modulo N;

first register means for providing constants 2^{+2mk} mod N and 1 as said input operands to said circuit;

second register means for storing the output from said circuit;

means for controlling input operand selection to said circuit so that after at most t iterations, the output result of said circuit is A^E modulo N.

7. An apparatus for computing A^E modulo N, where A, E and N are integers, with $A < 2N$, all having binary representations, and where n is the number of bits in the binary representation of N, and where $E = \sum_{i=0}^{t} e_i 2^i$, and where t is the number of bits in the binary representation of E, and where m and k are two positive integers such that $mk \geqslant n + 2$, said apparatus comprising:

a modular multiplication circuit having two input operands for signals representing binary numbers F and G and which produces as a result the binary representation of $F\,G\,2^{-mk}$ modulo N;

a first multiplexor for selecting input signals for a first one of said input operands to said modular multiplication circuit;

a second multiplexor for selecting input signals for the second one of said input operands to said modular multiplication circuit;

a first output register;

a second output register;

a selector circuit for supplying the output from said modular multiplication circuit to either one or both of said first and second registers; and

means for controlling said first and second multiplexors and said selector circuit over repeated cycles to produce said A^E modulo N value in at least one of said output registers.

8. The apparatus of claim 7 in which said means for controlling is a finite state machine which switches states in dependence on the values e_i and on the value of a counter.

9. The apparatus of claim 8 in which said counter counts from 0 to t.

10. The apparatus of claim 8 in which said finite state machine further includes a one-bit register indicating first and second step states.